



Karthik S Arkasali

 [linkedin.com/in/karthik-s-arkasali/](https://www.linkedin.com/in/karthik-s-arkasali/)
 karthiksarkasali.github.io/karthik.github.io/

 Karthik.arkasali@gmail.com
 Mobile: +919606746816

PROFESSIONAL SUMMARY

Motivated cybersecurity professional with hands-on experience in incident response, threat detection, and cloud security. Skilled in leveraging SIEM tools like Splunk and ELK for real-time log analysis and automated alert management. Proficient in frameworks such as NIST CSF, ISO 27001, and MITRE ATT&CK, with demonstrated success in implementing proactive incident response workflows. Completed certifications in Google Cloud Cybersecurity, gaining expertise in vulnerability management and risk mitigation. Adept at identifying security gaps, enhancing threat detection, and contributing to robust security defenses in dynamic SOC environments.

EDUCATION

Sapthagiri College of Engineering
Bachelors of Electronics & Communication

Bengaluru, India
Sep 2018 - August 2023

SKILLS SUMMARY

- **Languages:** Python, SQL
- **Networking:** OSI & TCP/IP Model, Firewall Configurations, Packet analysis with Wireshark
- **Security:** Incident Response, Log analysis, Threat Detection, Vulnerability Assessment, Risk Management
- **Frameworks:** NIST CSF, SOC, ISO 27001, MITRE ATT&CK, PCI DSS, HIPAA
- **Tools:** Splunk, ELK Stack, Tines, Shuffle, LimaCharlie, Nessus, Security Command Center, Google Cloud Console
- **Soft Skills:** Problem-Solving, Collaboration, Adaptability, Excellent communication

PROJECTS

- Respond and recover from a Data Breach (GCP) | [LINK](#) | [Document](#)** **January 2025**
- Analyzed a data breach by gathering critical information to assess the scope and impact of the incident.
 - Fixed vulnerabilities in Google Cloud Compute Engine, including deleting the compromised VM and securing access.
 - Corrected Cloud Storage bucket permissions to ensure proper access controls and secure data.
 - Enhanced firewall security by customizing firewall rules, restricting SSH access, enabling logging, and verifying compliance with industry standards.
- SOC Automation with ELK and Incident Response | [LINK](#) | [Workflow](#) | [Document](#)** **October 2024**
- Improved containment times and reduced alert analysis time through the implementation of real-time monitoring dashboards.
 - Set up and deployed the ELK stack (Elasticsearch, Logstash, Kibana) for centralized log monitoring and efficient alerting.
 - Simulated cyberattacks using Mythic C2 to validate and enhance threat detection and response processes.
 - Streamlined incident response by integrating a ticketing system to automate alert investigation and improve workflows.
- Automated Incident Response with LimaCharlie and SOAR Integration | [LINK](#) | [Workflow](#) | [Playbook](#)** **September 2024**
- Improved detection accuracy and accelerated incident response by implementing automated Slack and email notifications with decision workflows.
 - Configured LimaCharlie to analyze threat telemetry and create custom rules for real-time detection and response.
 - Developed an incident response playbook with user-friendly workflows to enable swift isolation of compromised machines.
 - Integrated Slack, email, and Tines to streamline Security Orchestration, Automation, and Response (SOAR) capabilities.

CERTIFICATES

- Google Cloud Cybersecurity (Google Cloud) | [CERTIFICATE](#)** **January 2025**
- Completed the Google Cloud Cybersecurity Certificate, covering cloud security, risk management frameworks (HIPAA, NIST CSF, SOC), and incident response.
 - Gained hands-on experience in attack mitigation, logging, monitoring, and vulnerability identification through practical applications.
- Google Cybersecurity (Coursera) | [CERTIFICATE](#)** **February 2024**
- Gained practical experience in Python, Linux, and SQL to develop and implement cybersecurity solutions.
 - Learned to identify and mitigate Risks, Threats, and Vulnerabilities while utilizing SIEM tools for network and data protection.

EXTRACURRICULAR / CERTIFICATES

- Commonwealth Bank Introduction to Cybersecurity Job Simulation on Forage | [CERTIFICATE](#) | [Document](#)** **October 2024**
- Gained hands-on fraud detection experience at Commonwealth Bank, developing Splunk dashboards and demonstrating incident response, including attack containment and recovery.
 - Designed infographics on secure password management based on Australian Cybersecurity Centre guidelines and conducted penetration testing to identify web application vulnerabilities, offering remediation recommendations.
- Mastercard Cybersecurity virtual experience program on Forage | [CERTIFICATE](#) | [Document](#)** **July 2024**
- Completed a job simulation where I served as an analyst on Mastercard's Security Awareness Team.
 - Identified areas needing stronger security training and implemented targeted courses and procedures.